REMARKS

The Office Action, mailed September 19, 2006, considered and rejected claims 1-24. Claims 1, 5-7, 11-13, 17-19, 23 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Andersson* (U.S. Patent No. 6,047,194) in view of *Moore* (U.S. Patent No. 5,475,374). Claims 2 and 14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Andersson* in view of *Moore*, and further in view of *Lager* (U.S. Patent No. 6,636,502). Claims 3, 4, 8, 15, 16 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Andersson* in view of *Moore*, and further in view of *Wang* (U.S. Patent No. 6,614,774). Claims 9 and 21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Andersson* in view of *Moore* and *Wang*, and further in view of *Brothers* (U.S. Patent No. 6,822,955).[1] Claims 10 and 22 were objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

By this paper, claims 1, 13, and 23 have been amended, while no claims have been added or cancelled.[2] Accordingly, following this paper, claims 1-24 remain pending, of which claims 1, 13 and 23 are the only independent claims at issue.

As reflected in the above claims, the present invention is generally directed to methods and systems for transmitting packet data in a way that ensures that pushed packet data is received only from desired originators. As reflected in claim 1, which recites a method from the perspective of a wireless mobile communication station which is the target of pushed packet data, the wireless mobile communication station receives a network address of an originator of packet data that is trying to push the data to the mobile communication station, where the originator is attempting to push the packet data to the wireless mobile communication station. The received network address is then compared with one or more predefined network addresses stored in the wireless mobile communication station to determine if the received network address matches an address corresponding to a predefined, authorized originator of packet data. If a match is made, the identity

---

[1] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should the need arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[2] Applicant notes that the remarks and amendments presented herein have been made merely to clarify the claimed embodiments and to explicitly recite elements that Applicant believes were already inherently present in the claims. For example, claims 1, 13 and 20 have been amended to clarify that the set of one or more predefined network addresses "correspond[] to one or more predefined originators of packet data" and that packet data is transmitted "from the originator" for receipt by the wireless communication station only *after* it is first determined that a received network address is included in the set of one or more predefined network addresses stored by the wireless communication station. Support for the claim amendments can be found throughout Applicant's application, including, but not limited to, the previously presented claims and the disclosure in original paragraphs 42, 50, and 53-55, and in Figures 1 and 2.

of the originator is also verified at the wireless mobile communication station and a packet data session with the originator is thereafter established as authentic. Thus, packet data is transmitted from the originator and received by the wireless mobile communication station only after determining that the received network address is in the set of predefined network addresses.

Claims 13 and 23 recite a method and system respectively, which implement a method generally corresponding to the method of claim 1 from the perspective of a system that includes an originator of push packet data and the wireless mobile communication station.

Applicant respectfully submits that the claims, particularly as clarified by the above claim amendments, define methods which are substantially different from the method or system of *Andersson*, whether alone or in combination with *Moore*. For example, among other things, *Andersson* and *Moore* fail to disclose or suggest a method or system in which a wireless mobile communication station establishes a packet data session with the originator, only after the identity of the originator is first verified as authentic, and such that the packet data is transmitted from the originator after the wireless mobile communication station determines that the received network address is included in a set of one or more predefined network addresses, as recited in the claims in combination with the other recited claim elements.

In fact, upon a review of the entirety of the *Andersson* reference, it appears that *Andersson* teaches the opposite of the claimed invention insofar as *Andersson* teaches that the packet data is transmitted from the originator of the packet data as the first step of the method, before the wireless device is even aware of the address of the incoming packet data. Accordingly, *Andersson* clearly fails to teach or suggest that the packet data session is only established after first authenticating the originator of the packet through the use of one or more predefined network addresses.

In particular, *Andersson* discloses methods and systems in which an Internet host originates packet data to be transmitted to a mobile terminal 14 for selective receipt by the mobile terminal. (Col. 5, ll. 5-9, 64-67). To implement *Andersson's* method of selectively receiving the packet data, "[f]irst…packet data originated at the Internet host 12 is routed by way of the Internet backbone 22 and received at the GPMSC 46" within a PLMN18, which packet data is then encapsulated and forwarded to a SMS-C 56 within the PLMN. (Col. 7, ll. 14-27, 36-54; Col. 8, ll. 44-53). The originated packet data sent from the Internet host includes the Internet host's source IP address, the host name, the service type, and the IP address associated with the wireless terminal. (Col. 7, ll. 23-26, 48-52). Using this information, an SMS message is generated and sent to the mobile terminal, which displays a message identifying the originator of the packet data, thereby allowing the user of

the mobile terminal to determine whether to permit transmission of the packet data to the mobile terminal. (Col. 7, ll. 42-64; Col. 8, ll. 21-40). If the user selects to receive the message, the mobile terminal registers to enter packet state so as to receive the packet data, and the PLMN forwards the packet data to the mobile terminal. (Col. 8, ll. 7-13, 40-43).

Thus, while *Andersson* appears to disclose a method in which messages are selectively received by a mobile device in response to a user indicating whether a message from a displayed source should be received, *Andersson* also discloses that the originating Internet host sends the package data before such selection is made by a user, and regardless of whether the user ultimately accepts the message, or whether the sender is first authenticated. In fact, *Andersson* expressly discloses that the originating Internet host's sending of the packet data directed to the wireless terminal is the first step in selectively routing the packet data to the mobile terminal. Stated another way, *Andersson* discloses that the PLMN transmits the packet data to the mobile device after receipt of permission from the user; however, the packet data is transmitted from the originating Internet host **before** any address is reviewed by the PLMN, before any determination is made as to whether the mobile terminal is to receive the packet data, and even before the targeted mobile device is identified by the PLMN. Moreover, as illustrated in Figure 2, this initial transmission of packet data from the originating Internet host appears to be the only time data is transmitted by the Internet host.

Thus, *Andersson* fails to teach or suggest wherein the originator transmits the packet data for receipt by a wireless mobile communication station only after it has been determined that a received network address is included in the set of one or more predefined network addresses stored by the wireless station.

Applicant also respectfully submits that *Moore* fails to disclose or suggest a wireless mobile communication station establishing a packet data session with the originator, after the identity of the originator is verified as authentic, and such that the packet data is transmitted from the originator after the wireless mobile communication station determines that the received network address is included in a set of one or more predefined network addresses, as recited in combination with the other claim elements. In particular, *Moore* discloses a method for conserving power in a mobile device which includes, upon turning the mobile device on, first receiving a message which includes address information and a long information portion. (Col. 5, ll. 37-41, 60-64; Col. 7, ll. 23-30). Thus, the message disclosed in *Moore* is transmitted in the first instance, before any addresses are used in any manner.

Additionally, neither *Andersson* nor *Moore* discloses or suggests a method or system in which the set of one or more predefined network addresses, to which the received network address is matched, correspond to predefined originators of packet data, as recited in combination with the other claim elements. In fact, as acknowledged by in the Office Action, *Andersson* is devoid of any teaching regarding a set of one or more predefined network addresses stored in the mobile device. (Office Action, p. 4). Instead, as noted above, the original packet from the originating Internet host sends packet information which identifies the Internet host by its IP address and name, and thereafter displaying that information to the user for the user to authenticate. Accordingly, for at least this reason, the Examiner relies upon *Moore*.

Applicant respectfully submits, however, that *Moore* fails to remedy the foregoing inadequacies of *Andersson*. Instead, *Moore* discloses a system in which an initial message is sent to a portable telephone device and includes a synchronization portion, an index portion, an information portion, and an optional address portion. (Col. 5, ll. 37-46). In the address portion, "selective call or group call addresses" are included which indicate "which portable device or group of portable devices operating in the radio communication system, are intended to further process information within the message," and to "identify particular groups or <u>receivers</u> which process the messages." (Col. 5, ll. 48-52; Col. 5, ln. 67 to Col. 6, ln. 3). This information is then compared to selective call or group call addresses" (i.e. identifications of receivers) in the portable device. (Col. 5, ll. 53-56; Col. 7, ll. 31-36; Col. 8, ll. 63-66). Thereafter, upon determining that the address of the message matches the addresses of the portable device, a low power mode can be scheduled. (Col. 8, ln. 6 to Col. 9, ln. 4).

Thus, while *Moore* discloses sending messages with addresses and comparing the addresses to stored addresses, *Moore* discloses that the addresses identify <u>receivers</u> which will process the messages, but does not disclose that the message identifies any <u>originator</u> of packet data as claimed in combination with the other claim elements. Thus, Applicant respectfully disagrees with the assertion of the Office Action that address 410 is "of a caller". In particular, as discussed above, and as expressly recited in *Moore*, instead of an address of the originator of packet data, the addresses in *Moore* are "a group call or an all call address, intended to identify particular groups of <u>receivers</u> which process the messages." Thus, inasmuch as *Moore* teaches comparing addresses of receivers of messages, rather than an originator of the message, *Moore* also fails to teach a set of one or more predefined network addresses corresponding to one or more predefined originators of packet data as recited in combination with the other claim elements.

For at least these reasons, Applicant respectfully submits that the independent claims are therefore distinguished from the art of record, and reconsideration of the above claims is respectfully requested. In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice.[3] Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 13th day of March, 2007.

Respectfully submitted,

JENS C. JENKINS
Registration No. 44,803
COLBY C. NUTTALL
Registration No. 58,146
Attorneys for Applicant
Customer No. 22913

RDN:JCJ:CCN:crb
AHY0000002999V001

---

[3] For example, among other assertions made in the Office Action, Applicant does not acquiesce to the apparent assertion of the Office Action that Applicant, in paragraph [0045] of the original specification, discloses that "determining if the received network address matches a predefined network address of the originator that is included in a set of one or more predefined network addresses stored by the wireless mobile communication station" is performed manually by a user. For example, paragraph [0045] notes that manual verification by a user is an alternative to the application checking a host name and comparing it with the stored server host name. Moreover, paragraph [0045] relates to authenticating the push server by examining the "host name" obtained after a DNS server has looked up the domain name corresponding to a previously received IP address of the push server, while original paragraph [0042] discloses a received IP address being compared against a set of stored IP addresses.